IN THE CLAIMS

4. (Three Times Amended) A [cryptographic] system for communications [system] of a message cryptographically processed with an RSA public key encryption comprising:

a communication [medium] channel for transmitting a ciphertext word signal C;

[an] encoding means coupled to said channel and adapted for transforming a transmit message word signal M to [a] the ciphertext word signal C [and for transmitting C on said channel, where M corresponds to a number representative of a message and $0 \leq M \leq n-1$ where n is a composite number] using a composite number, n, where n is a product of the form

$$n=p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

[where] k is an integer greater than 2, and $p_1, p_2, \ldots, p_k$ are distinct random prime numbers, [and] where [C] the transmit message word signal M corresponds to a number representative of [an enciphered form of said] the message and [corresponds to] $0 \leq M \leq n-1$

where the ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

[$C \equiv M^e \pmod n$] $C \equiv M^e \pmod n$, and

where e is a number relatively prime to $\text{lcm}(p_1-1, p_2-1, \ldots, p_k-1)$; and

[a] decoding means coupled to said channel and adapted for receiving the ciphertext word signal C from said channel and, having available to it the k distinct random prime number $p_1, p_2, \ldots p_k$, for transforming the ciphertext word signal C to a receive message word signal M' where M' corresponds to a number representative of a [deciphered] decoded form of the ciphertext word signal C [and corresponds to] through a relationship of the form

[$M' \equiv C^d \pmod n$] $M' \equiv C^d \pmod n$

where d is selected from the group consisting of [the] a class of numbers equivalent to a multiplicative inverse of

$$e(\text{mod}(\text{lcm}((p_1-1), (p_2-1), \ldots, (p_k-1))))).$$

7. Cancelled

13. Cancelled

New Claims:

35. (Twice Amended) The method according to claim [[14]] 9, wherein [[a]] the signed message word signal M_{1s}, formed from the digital message word signal M_1 being cryptographically processed [in accordance with the method is compatible with two-prime] at the fist terminal with multi-prime (k>2) RSA public key [cryptography] encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, ... [[pk]] p_k, is decipherable at the second terminal with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q.